



IP WAN Checklist V 2.3

12 August 2005

Developed by DISA for the DOD

Database Reference Number: _____

Database entered by: _____ Date: _____

Technical Q/A by: _____ Date: _____

Final Q/A by: _____ Date: _____

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

FOUO UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Enclave Reviewer				Phone			
Previous SRR	Y	N	Date of Previous SRR		S01 Available	Y	N
Number of Current Open Findings							

Site Name			
Address			
Phone			

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

3 - IP WAN Configuration Management and Operational Standards

IPW0010

Severity: CAT II

STIG Ref:

3

Policy: The IP WAN program office will establish and document an IP WAN configuration management process.

Procedure: Interview the IAO and verify a documented configuration management process.

Reference: DODI 8500.2 DCPR-1, DCCB-2

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3 - IP WAN Configuration Management and Operational Standards

IPW0020

Severity: CAT II

STIG Ref:

3

Policy: The IP WAN IAOs will be a voting member of the configuration management process to ensure adherence to the security requirements of the IP WAN STIG.

Procedure: Interview the IAO and verify the IAO is a CCB member with voting privileges.

Reference: DODI 8500.2 DCPR-1, DCCB-2

Category: Configuration Control/Management Board

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3 - IP WAN Configuration Management and Operational Standards

IPW0030

Severity: CAT III

STIG Ref:

3

Policy: The IP WAN PMO will ensure the IP WAN TNC IAMs are aware of the configuration management process and adhere to the documented configuration management process.

Procedure: Interview the IAM to verify compliance with the Configuration management process.

Reference: DODI 8500.2 PRTN-1, DCPR-1

Category: Configuration Control/Management Board

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.1 - Documentation Management

IPW0040

Severity: CAT II

STIG Ref:

3.1

Policy: The IP WAN TNC will create and maintain topology diagrams to be used by the TNC, the IP WAN PMO, and the IP WAN GNSC.

Procedure: Review the IP WAN topology diagrams and verify their accuracy by reviewing a sampling of device physical and logical configurations.

Reference: DODI 8500.2 DCHW-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.2 - Standard Operating Procedures

IPW0050

Severity: CAT II

STIG Ref:

3.2

Policy: The IP WAN Program Office will ensure the following standard operating procedure(s) (SOP) is maintained for all network devices:

- Software version control and management
- IP addressing standards and management
- Naming conventions and Domain Name System (DNS) assignments
- Configuration upgrade procedures
- Procedures for Issuance of emergency passwords

Procedure: Interview the IAO and verify SOPs exist.

Reference: DODI 8500.2 DCPR-1

Category: Procedures and Policies

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.2 - Standard Operating Procedures

IPW0060

Severity: CAT II

STIG Ref:

3.2

Policy: The IP WAN PMO will document all deviations to the baseline configuration and will ensure the IP WAN CCB approves them.

Procedure: Interview the IAO and verify that recent changes have been documented and approved by the CCB.

Reference: DODI 8500.2 DCCB-2

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.2 - Standard Operating Procedures

IPW0070

Severity: CAT II

STIG Ref:

3.2

Policy: The IP WAN Program Office will create and maintain testing procedures for all new or upgraded hardware and software.

Procedure: Interview the IAO to verify testing procedures exist and are used prior to implementing new devices on the network.

Reference: DODI 8500.2 DCCT-1

Category: Procedures

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.2 - Standard Operating Procedures

IPW0080

Severity: CAT III

STIG Ref:

3.2

Policy: The IP WAN PMO will provide documented procedures for MD5 key management to include: key exchange, the use of key chains, length, key compromise, and storage.

NOTE: MD5 keys must be changed at least every six months for Interior Gateway Protocols (IS-IS, EIGRP, OSPF) and at least every year for Interior Border Gateway Protocol (IBGP) and External Border Gateway Protocol (EBGP).

Procedure: Interview the IAO to verify that MD5 key management procedures exist and are used.

Reference: DODI 8500.2 IAKM-2

Category: Procedures

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.3 - Change Control

IPW0090

Severity: CAT II

STIG Ref:

3.3

Policy: The IP WAN Program Office will document and maintain baseline configurations for all IP WAN devices.

Procedure: Interview the IAO to verify that baseline configurations for all IP WAN devices documented and maintained.

Reference: DODI 8500.2 DCSW-1

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.3 - Change Control

IPW0100

Severity: CAT IV

STIG Ref:

3.3

Policy: The IAO will ensure the current and previous router configurations are stored in a location that restricts access to authorized users.

Procedure: Interview the IAO or the router administrator and verify that a current copy of the configuration exists in a backup file and that an archived configuration exists.

Reference: DODI 8500.2 COSW-1

Category: Backup and Recovery Procedures

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.4 - Device Operating System Version Control

IPW0110

Severity: CAT II

STIG Ref:

3.4

Policy: The IP WAN IAO will ensure PMO directed software versions are installed.

Procedure: Verify that current software versions are recommended and approved for use by the PMO.

Reference: DODI 8500.2 DCCT-1

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.5 - Upgrade / Release Control

IPW0120

Severity: CAT IV

STIG Ref:

3.5

Policy: The IP WAN PMO will develop procedures for deploying new software and upgrading deployed software.

Procedure: Interview the IAO. Review software upgrade and deployment procedures to ensure testing, distribution, management, and recovery items are addressed.

Reference: DODI 8500.2 DCCT-1

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.5 - Upgrade / Release Control

IPW0130

Severity: CAT IV

STIG Ref:

3.5

Policy: The IP WAN PMO software upgrade and release procedures will define all steps for the upgrade, reference vendor documentation related to updating the device, and provide testing procedures for validating the upgrade was successful.

Procedure: Interview the IAO. Review the Software Upgrade and Release Procedures or comparable documentation to ensure the integrity and reliability of an upgrade is maintained and verified during an upgrade.

Reference: DODI 8500.2 DCPR-1

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.5 - Upgrade / Release Control

IPW0140

Severity: CAT II

STIG Ref:

3.5

Policy: The IP WAN PMO will ensure once upgrade procedures are defined and validated, the upgrade procedure will be referenced in all change documentation appropriate to the particular upgrade.

Procedure: Interview the IAO and review a sampling of recent change documentation or instructions.

Reference: DODI 8500.2 DCPR-1, DCCT-1

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.5 - Upgrade / Release Control

IPW0150

Severity: CAT III

STIG Ref:

3.5

Policy: The IP WAN IAO will ensure only authorized IP WAN router administrators are given access to stored configuration files.

Procedure: Interview the IAO. Verify that access controls are in place to prevent unauthorized users from accessing stored configuration files or folders.

Reference: DODI 8500.2 ECCD-1, ECCD-2, ECLP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.5 - Upgrade / Release Control

IPW0160

Severity: CAT II

STIG Ref:

3.5

Policy: The IP WAN router administrators will not store unencrypted router passwords in an offline configuration file.

Procedure: Interview the IAO and verify the procedure to store offline configuration files with encrypted passwords.

Reference: DODI 8500.2 ECCR-1

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.6 - Vulnerability Management

IPW0170

Severity: CAT IV

STIG Ref:

3.6

Policy: The IAO will ensure all System Administrators (SAs) that are responsible for IP WAN information systems are registered in VMS.

Procedure: Interview the IAO to verify that SAs are registered in VMS.

Reference: DODI 8500.2 VIVM-1

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.6 - Vulnerability Management

IPW0180

Severity: CAT II

STIG Ref:

3.6

Policy: The IP WAN SA will ensure all IP WAN devices are IAVA compliant prior to connecting the device to the IP WAN.

Procedure: Interview the IAO to determine compliancy.

Reference: DODI 8500.2 ECND-2

Category: IAVA Alerts

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.6 - Vulnerability Management

IPW0190

Severity: CAT III

STIG Ref:

3.6

Policy: The IAO in coordination with the SA, will ensure all IAVM notices are responded to within the specified time period.

Procedure: Interview the IAO. Verify applicable IAVM messages have been addressed within appropriate time frames.

Reference: DODI 8500.2 ECND-2

Category: IAVA Alerts

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.7 - Asset Management

IPW0200

Severity: CAT II

STIG Ref:

3.7

Policy: The IP WAN SA will properly register and manage all IP WAN assets in the Vulnerability Compliance Tracking System (VCTS) portion of the Vulnerability Management System (VMS).

Procedure: Interview the IAO. Review VCTS registered assets against system documentation and inventory.

Reference: DODI 8500.2 ECND-2

Category: Configuration Management

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.8 - DOD Port, Protocols, and Services (PPS)

IPW0210

Severity: CAT II

STIG Ref:

3.8

Policy: The IP WAN router administrators will ensure IP WAN devices are configured IAW the DODI 8551.1.

Procedure: Review access control lists and compare against the most recent published DOD Ports, Protocols, and Services guidance.

Reference: DODI 8500.2 DCP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

3.8 - DOD Port, Protocols, and Services (PPS)

IPW0215

Severity: CAT III

STIG Ref:

3.8

Policy: The IP WAN PMO will ensure the ports, protocols, and services used by all IP WAN devices are registered in the PPS Registry. (This includes the PPS's used for network management and troubleshooting of IP WAN devices.)

Procedure: Interview the IP IAO to determine if a process exists to register PPSs in the PPS Registry. Have the IAO log on to the PPS Registry and request to see their registered applications.

Reference: DODI 8500.2 DCP-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.1 - Secure Shell (SSH)

IPW0220

Severity: CAT III

STIG Ref:

4.1

Policy: The IP WAN IAM will ensure all workstations used to remotely manage IP WAN communication devices have an SSH client installed.

Procedure: Interview the IAO. Verify that remote management workstations have authorized SSH clients installed.

Reference: DODI 8500.2 ECK-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.2 - File Transfer Services

IPW0230

Severity: CAT III

STIG Ref:

4.2

Policy: The IP WAN router administrator will ensure all file transfer servers are secured IAW the appropriate Operating System STIG (i.e., UNIX, Windows)

Procedure: Interview the IAO and the SA to verify the guide(s) that were used to configure the security settings on the file transfer server.

Reference: DODI 8500.2 DCCS-2

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.2 - File Transfer Services

IPW0240

Severity: CAT I

STIG Ref:

4.2

Policy: The IP WAN router administrator will ensure device user account and passwords and/or SNMP community strings are not stored in clear text, to include automated scripts.

Procedure: Verify stored files do not contain clear text passwords or SNMP community strings.

Reference: DODI 8500.2 ECCR-2, IAIA-1

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0250

Severity: CAT II

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) is used across the entire network infrastructure.

Note: If a device does not support SNMPv3, SNMPv2 may be used if access control mechanisms are to ensure only authorized SNMP clients and servers can communicate with each other.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0260

Severity: CAT II

STIG Ref:

4.3

Policy: If SNMPv2C is used, the IP WAN IAO will ensure the community strings are protected from compromise (i.e., encrypt stored files that contain the community strings).

Procedure: Verify stored files do not contain SNMP community strings.

Reference: DODI 8500.2 ECCR-2, IAIA-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0270

Severity: CAT II

STIG Ref:

4.3

Policy: The IAO will establish and maintain a standard operating procedure (SOP) for SNMP community string management to include the following:

* SNMP string expiration or account expiration

* SNMP account credentials (i.e., user id, password, community string) will be created IAW DODI 8500.2 IAIA-1.

* SNMP community distribution including determination of membership

Procedure: Interview the IAO. Review their documented procedures.

Reference: DODI 8500.2 IA1A-1, IA1A-2

Category: Network and Communications Security

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.3 - SNMP

IPW0280

Severity: CAT III

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure if both privileged and non-privileged modes are used on all devices, that different community names are used for read-only access and read-write access.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECLP-1

Category: Access Controls

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.3 - SNMP

IPW0290

Severity: CAT II

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure SNMP servers and/or NMS systems restrict access to authorized IP addresses (i.e., ACL based on source and destination address and ports of IP WAN communication devices authorized to communicate with the server).

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.3 - SNMP

IPW0300

Severity: CAT III

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure security alarms are set up within the managed network's framework. At a minimum, the configured alarms are to include the following:

- * Integrity Violation: Indicates that network contents or objects have been illegally modified, deleted, or added.
- * Operational Violation: Indicates that a desired object or service could not be used.
- * Physical Violation: Indicates that a physical part of the network (such as a cable) has been damaged or modified without authorization.
- * Security Mechanism Violation: Indicates that the network's security system has been compromised or breached.
- * Time Domain Violation: Indicates that an event has happened outside of its allowed or normal time slot.

Procedure: Request that the network engineer demonstrate the alert capabilities.

Reference: DODI 8500.2 DCBP-1

Category: Monitoring

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.3 - SNMP

IPW0310

Severity: CAT III

STIG Ref:

4.3

Policy: The IP WAN NSO will ensure alarms are categorized by severity using the following guidelines:

- * Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that has been lost completely.
- * A major alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.
- * A minor alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.
- * A warning alarm is used to signal a potential problem that may affect service.
- * An indeterminate alarm is one that requires human intervention to decide its severity.

Procedure: Request that the network engineer demonstrate the alert capabilities.

Reference: DODI 8500.2 DCBP-1

Category: Monitoring

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.3 - SNMP

IPW0320

Severity: CAT II

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure the management workstation is located in a secure environment approved for at least secret level processing.

Procedure: Inspect the location of the network management workstations.

Reference: DODI 8500.2 PEPF-1, PEPF-2

Category: Network and Communications Security

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.3 - SNMP

IPW0330

Severity: CAT II

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure only accounts necessary for the operation of the system and for access logging are enabled.

Procedure: Review the configuration of the NMS with the IAO to verify that proper account administration is being enforced. Review the accounts and the personnel using them to verify that they require access.

Reference: DODI 8500.2 IAAC-1

Category: User-ID Administration

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0340

Severity: CAT III

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure a record is maintained of all logons and transactions processed by the management station, to include log in and log out times, devices that were accessed and modified, and configuration read and write events.

Procedure: Review the NMS configuration and logs

Reference: DODI 8500.2 ECAR-1, ECAR-2, ECAR-3

Category: Accounting Data and Resources

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0350

Severity: CAT I

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure only authorized users can access the NMS.

Procedure: Review the NMS configuration to verify compliancy.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0360

Severity: CAT II

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure access controls are configured to only permit remote connections to the NMS from approved monitored/managed devices.

Procedure: Review the NMS configuration to verify compliancy.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0370

Severity: CAT II

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure all NMS user accounts are assigned the lowest level of access/rights necessary to perform their job function.

Procedure: Review the NMS configuration to verify compliancy.

Reference: DODI 8500.2 ECLP-1

Category: Group User-IDs

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0380

Severity: CAT I

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure default passwords on the SNMP servers and NMS servers are changed during initial configuration, prior to being deployed, and that the strings comply with the password standards as defined in DODI 8500.2, IAIA-1.

Procedure: Interview the IAO. With permission from then IAO, attempt to logon to some of the devices.

Reference: DODI 8500.2 IAIA-1

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.3 - SNMP

IPW0385

Severity: CAT II

STIG Ref:

4.3

Policy: The IP WAN IAO will ensure the SNMP servers and NMS are configured IAW the appropriate Operating System STIG(s).

Procedure: Interview the IAO to determine if a recent SRR has been performed for the NMS and if it is compliant.

Reference: DODI 8500.2 DCCS-1, DCCS-2

Category: Operating System Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.4 - SYSLOG

IPW0390

Severity: CAT IV

STIG Ref:

4.4

Policy: The IP WAN NSO will ensure a centralized syslog server is deployed and configured to receive all syslog messages. Syslog messages must be retained for one year; a minimum of 30 days must be stored online.

Procedure: Examine the syslog server to verify that it is configured to store messages for at least 30 days. Have the administrator show you the syslog files stored offline for one year.

Reference: DODI 8500.2 ECTB-1

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.4 - SYSLOG

IPW0400

Severity: CAT III

STIG Ref:

4.4

Policy: The IP WAN syslog administrator will secure the syslog server IAW the appropriate Operating System STIG(s).

Procedure: Interview the IAO to determine if a recent SRR has been performed for the syslog server and if it is compliant.

Reference: DODI 8500.2 DCCS-1, DCCS-2

Category: Operating System Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.4 - SYSLOG

IPW0410

Severity: CAT IV

STIG Ref:

4.4

Policy: The IP WAN syslog administrator will configure the syslog server to accept messages from only authorized devices (i.e., restricting access via source and destination IP address).

Procedure: Review the syslog server configuration to determine if there is filtering (ACL or TCP wrappers) that will limit access.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5 - AAA

IPW0420

Severity: CAT III

STIG Ref:

4.5

Policy: The IP WAN router administrators will ensure configuration changes are logged to the syslog server with the logon account name that made the change.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECTB-1

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5 - AAA

IPW0430

Severity: CAT II

STIG Ref:

4.5

Policy: The IP WAN router administrators will ensure the AAA log creates an audit trail of activity. The audit logs will be stored for one year, online for a minimum of one month and offline for a minimum of eleven months. The log will be configured, at a minimum, to log the following events:

- * Username
- * Time-Stamp
- * Network device being managed
- * Privilege level assigned
- * Severity Code

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECTB-1

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.1 - AAA - Router Management User Accounts

IPW0440

Severity: CAT III

STIG Ref:

4.5.1

Policy: The IP WAN IAO will ensure a DOD Form 2875 is used to validate user requirements and authorizations for router management account requests and to determine proper authorization privileges.

Procedure: Interview the IAO.

Reference: DODI 8500.2 PRAS-1, PRAS-2

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.1 - AAA - Router Management User Accounts

IPW0450

Severity: CAT I

STIG Ref:

4.5.1

Policy: The IP WAN IAO will ensure only authorized users are configured in the AAA server.

Procedure: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts found in the router's local database or AAA server.

Reference: DODI 8500.2 IAAC-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.1 - AAA - Router Management User Accounts

IPW0460

Severity: CAT I

STIG Ref:

4.5.1

Policy: The IP WAN IAO will ensure individual user accounts with unique passwords are configured in the AAA server.

Procedure: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts found in the router's local database or AAA server.

Reference: DODI 8500.2 IAAC-1

Category: Group User-IDs

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.1 - AAA - Router Management User Accounts

IPW0470

Severity: CAT II

STIG Ref:

4.5.1

Policy: The IP WAN IAO will disable or remove expired or dormant IP WAN router management user accounts.

Procedure: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts found in the router's local database or AAA server.

Reference: DODI 8500.2 IAAC-1

Category: Access Controls

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.5.1 - AAA - Router Management User Accounts

IPW0480

Severity: CAT II

STIG Ref:

4.5.1

Policy: The IP WAN IAO will ensure each router management user account is assigned to an AAA authorization group with the lowest privileges that permit the user to perform their job.

Procedure: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts found in the router's local database or AAA server. Reference the appropriate router checklist procedure guide when reviewing local accounts.

Reference: DODI 8500.2 IAAC-1

Category: User-ID Attributes

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.5.1 - AAA - Router Management User Accounts

IPW0490

Severity: CAT II

STIG Ref:

4.5.1

Policy: The IP WAN IAO will ensure router management accounts are configured to use two-factor authentication for all router management connectivity (i.e., SSH to router or local connection to console).

Procedure: Interview the IAO and router administrator for compliance. Have the router administrator establish a management session to determine compliance. Review the authentication server configuration.

Reference: DODI 8500.2 IAAC-1, IAIA-1, IAIA-2

Category: Network and Communications Security

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

4.5.2 - AAA - TACACS+

IPW0500

Severity: CAT III

STIG Ref:

4.5.2

Policy: The IP WAN TACACS+ SA will ensure the TACACS+ server is configured IAW the appropriate Operating System STIG.

Procedure: Interview the IAO to determine if a recent SRR has been performed for the authentication server and if it is compliant.

Reference: DODI 8500.2 DCCS-1, DCCS-2

Category: Operating System Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.2 - AAA - TACACS+

IPW0510

Severity: CAT III

STIG Ref:

4.5.2

Policy: The IP WAN TACACS+ SA will create tiered authorization groups for router management accounts on the TACACS+ server

Procedure: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts found in the router's local database or AAA server.

Reference: DODI 8500.2 ECLP-1

Category: User-ID Attributes

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.2 - AAA - TACACS+

IPW0520

Severity: CAT III

STIG Ref:

4.5.2

Policy: The IP WAN router administrator will ensure access to the TACACS+ server is restricted to approved devices (i.e., firewall or router ACL that will only permit approved routers to connect with the TACACS+ server based on source and destination IP addresses and ports).

Procedure: Examine the network topology to determine where the authentication server resides. Verify that either a firewall, router ACL, host ACL or TCP wrappers insure that access to the authentication server is restricted to only authorized IP addresses.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.2 - AAA - TACACS+

IPW0530

Severity: CAT III

STIG Ref:

4.5.2

Policy: The IP WAN router administrator will ensure two or more TACACS+ servers are configured to support of device user authentication.

Procedure: Reference the appropriate router checklist procedure guide. Verify that both servers have been configured and are online.

Reference: DODI 8500.2 DCBP-1

Category: Backup and Recovery Procedures

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.3 - AAA - RADIUS

IPW0540

Severity: CAT III

STIG Ref:

4.5.3

Policy: The IP WAN router administrator will ensure the RADIUS server is configured IAW the appropriate Operating System STIG.

Procedure: Interview the IAO to determine if a recent SRR has been performed for the authentication server and if it is compliant.

Reference: DODI 8500.2 DCCS-1, DCCS-2

Category: Operating System Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.3 - AAA - RADIUS

IPW0550

Severity: CAT III

STIG Ref:

4.5.3

Policy: The IP WAN router administrator will ensure access to the RADIUS server is restricted to approved devices (i.e., firewall or router ACL that will only permit approved routers to connect with the RADIUS server based on source and destination IP addresses and ports).

Procedure: Examine the network topology to determine where the authentication server resides. Verify that either a firewall, router ACL, host ACL or TCP wrappers insure that access to the authentication server is restricted to only authorized IP addresses.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

4.5.4 - AAA - RSA SecurID

IPW0560

Severity: CAT III

STIG Ref:

4.5.4

Policy: The IP WAN IAO will ensure all RSA SecurID ACE servers are secured IAW the appropriate Operating System STIG.

Procedure: Interview the IAO to determine if a recent SRR has been performed for the RSA SecurID ACE server and if it is compliant.

Reference: DODI 8500.2 DCCS-1, DCCS-2

Category: Operating System Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.2 - OOB Communication Devices

IPW0570

Severity: CAT II

STIG Ref:

5.2

Policy: The IP WAN IAO will ensure OOBM connections are configured to use the following:

- * Authenticated access control
- * Two-factor authentication
- * Encryption of data in transit
- * Auditing of user sessions (on the AAA server or the OOB device)

Procedure: Interview the IAO and router administrator for compliance. Have the router administrator establish a OOBM session to determine compliance. Review the authentication server configuration.

Reference: DODI 8500.2 IAAC-1, IAIA-1, IAIA-2

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.3 - Communication Servers

IPW0580

Severity: CAT II

STIG Ref:

5.3

Policy: The IP WAN IAO will ensure management user account authentication is configured to use RADIUS or TACACS+ services.

Procedure: Interview the IAO and administrator for compliance. Have the administrator establish a management session with a communication servers to determine compliance.

Reference: DODI 8500.2 IAAC-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.3 - Communication Servers

IPW0590

Severity: CAT II

STIG Ref:

5.3

Policy: The IP WAN IAO will ensure communication servers are configured IAW the Remote Access Server/Network Access Server section of the Network Infrastructure STIG.

Procedure: Review the configuration for the RAS/NAS.

Reference: Network Infrastructure STIG 4.4, DODI 8500.2
EBRU-1 DCBP-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0600

Severity: CAT III

STIG Ref:

5.4.1

Policy: The IP WAN router administrator will ensure all communication devices are configured to use two or more TACACS+/RADIUS server hosts.

Procedure: Reference the appropriate router checklist procedure guide. Verify that both servers have been configured and are online.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0610

Severity: CAT III

STIG Ref:

5.4.1

Policy: The IP WAN router administrator will ensure all routers are configured to use AAA tiered authorization groups for remote management authentication.

Procedure: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts found in the router's local database or authentication server. Reference the appropriate router checklist procedure guide when reviewing local accounts.

Reference: DODI 8500.2 ECLP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0620

Severity: CAT III

STIG Ref:

5.4.1

Policy: The IP WAN router administrator will ensure all AAA authentication services are configured to use two-factor authentication during normal operation.

* Exception: Automated scripts are permitted to use single factor authentication accounts. Automated script user accounts should initiate a password change every thirty days.

Procedure: Interview the IAO and router administrator for compliance. Have the router administrator establish a management session to determine compliance. Review the authentication server configuration.

Reference: DODI 8500.2 IAAC-1, IAIA-1, IAIA-2

Category: Network and Communications Security

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

5.4.1 - Router - AAA

IPW0630

Severity: CAT II

STIG Ref:

5.4.1

Policy: The IP WAN router administrators will ensure only one local user account is set up on the router and that it will default to the lowest authorization level.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECPA-1

Category: Routers

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

5.4.1 - Router - AAA

IPW0640

Severity: CAT II

STIG Ref:

5.4.1

Policy: The IAO will ensure procedures exist and are practiced to securely control the creation, storage, and distribution of privileged local emergency user accounts.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECPA-1

Category: Routers

OPEN: ☐ NOT A FINDING: ☐ NOT REVIEWED: ☐ NOT APPLICABLE: ☐

NOTES:

5.4.1 - Router - AAA

IPW0650

Severity: CAT II

STIG Ref:

5.4.1

Policy: The IP WAN router administrators will create and maintain local emergency account passwords using password requirements as explained by the DODI 8500.2, IA controls IAIA-1 and IAIA-2.

Procedure: Interview the IAO and router administrator.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0660

Severity: CAT II

STIG Ref:

5.4.1

Policy: The IP WAN router administrators will ensure the enable secret password is verified locally in the event the AAA authentication service is not available.

Procedure: Review the authentication server configuration with the authentication server administrator to verify that the enable password is verified through the server. Have the router administrator sign onto the router directly and try to access the local enable password (should fail). Next have the administrator sign on through the authentication server and try to access the local enable password (should pass).

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0670

Severity: CAT I

STIG Ref:

5.4.1

Policy: The IP WAN Router Administrator will ensure the 'enable secret' command is used to protect the privileged access password.

Procedure: IOS Procedure: Review all Cisco router configurations to ensure an enable secret password is defined similar to the following example: enable secret 5 \$1\$rTsF\$EdvjtWbi0qA2gXwyhetTb1

JUNOS Procedure: This is NA for Juniper routers as there is no enable or privilege mode passwords or in the case of JUNOS, there is no password prompt to enter edit mode.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0680

Severity: CAT III

STIG Ref:

5.4.1

Policy: IP WAN router administrators will ensure the enable secret password does not match any other user password or any other enable secret password (i.e., each router has its own enable secret password).

Procedure: IOS Procedure: Interview the router administrators to see if this is being enforced on all Cisco routers.

JUNOS Procedure: This is NA for Juniper routers as there is no enable mode passwords, that is, there is no password prompt to enter edit or configuration mode.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0690

Severity: CAT II

STIG Ref:

5.4.1

Policy: The IP WAN router administrators will ensure the 'service password-encryption' option is used so that passwords will not be displayed in the clear.

Procedure: IOS Procedure: Examine all Cisco router configurations to determine if the global command service password-encryption is present.

JUNOS Procedure: For JUNOS, all passwords are always shown as encrypted; hence, this would never be a finding.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0700

Severity: CAT II

STIG Ref:

5.4.1

Policy: The IP WAN SA will ensure passwords are not stored in the clear. This includes back up files and automated management scripts.

Procedure: Interview the IAO and router administrator.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0710

Severity: CAT I

STIG Ref:

5.4.1

Policy: IP WAN router administrators will ensure standard or default vendor passwords are changed prior to connecting the device to the network.

Procedure: Interview the IAO and router administrator. With permission of the IAO or administrator, attempt to logon to the router.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.1 - Router - AAA

IPW0720

Severity: CAT II

STIG Ref:

5.4.1

Policy: The IP WAN router administrator will ensure the SNMP community strings and the RADIUS or TACACS+ key values do not equal any of the other passwords on the device.

Procedure: Interview the IAO and router administrator.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0730

Severity: CAT III

STIG Ref:

5.4.2

Policy: The IP WAN router administrator will ensure a loopback interface is configured on each router to be used for router management.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0740

Severity: CAT IV

STIG Ref:

5.4.2

Policy: The IP WAN router administrator will configure BGP updates to be sourced from the loopback interface (i.e., neighbor x.x.x.x update-source loopback 0).

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0760

Severity: CAT IV

STIG Ref:

5.4.2

Policy: The IP WAN router administrators will configure the loopback interface as the source address used for FTP access.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0770

Severity: CAT IV

STIG Ref:

5.4.2

Policy: The IP WAN router administrators will configure the routers to use the loopback interface as the source address for SNMP traps.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0780

Severity: CAT IV

STIG Ref:

5.4.2

Policy: The IP WAN router administrators will configure the routers to use the loopback interface as the source address when communicating with the TACACS+ or RADIUS servers.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0790

Severity: CAT IV

STIG Ref:

5.4.2

Policy: If Netflow is used on an IP WAN device, the IP WAN router administrator will configure the device to use the loopback interface as the source address for NetFlow traffic.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0800

Severity: CAT IV

STIG Ref:

5.4.2

Policy: If an IP WAN device provides NTP updates, the IP WAN SA will configure the device to use the loopback interface as the source address for NTP traffic.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0810

Severity: CAT IV

STIG Ref:

5.4.2

Policy: The IP WAN router administrators will configure the router to use the loopback interface as the source address for syslog traffic.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.2 - Router - Loopback Interfaces

IPW0820

Severity: CAT IV

STIG Ref:

5.4.2

Policy: The IP WAN router administrators will configure the routers to allow SSH connections to the loopback interface IP Address.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0830

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure Cisco Discovery Protocol (CDP) is disabled on all external Cisco router interfaces.

Procedure: Review all Cisco router configurations to ensure no cdp run is included in the global configuration or no cdp enable is included for each active external interface.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0840

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure TCP & UDP small services is disabled.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that service udp-small-servers and service tcp-small-servers are not found.

Note: The TCP and UDP small servers are enabled by default on Cisco IOS Software Version 11.2 and earlier. They are disabled by default on Cisco IOS Software Versions 11.3 and later.

JUNOS Procedure: JUNOS does not support the echo, chargen, discard or daytime services; hence, this will never be a finding.

Reference: DODI 8500.2 DCBP-1

Category: Service Configuration

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0850

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure PAD services are disabled.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that the no service pad command is configured or that the service pad command is not found.

JUNOS Procedure: JUNOS does not support PAD services; hence, this will never be a finding.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0860

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure TCP keep-alives for telnet sessions are enabled.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that the following IOS commands have been configured:

service tcp-keep-alives in
service tcp-keep-alives out

JUNOS Procedure: NA

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0870

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure DHCP services is disabled.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that no service dhcp is found.

Note: Service DHCP is enabled by default.

JUNOS Procedure: NA

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0880

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure Finger services are disabled.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that the IOS command, no ip finger for IOS version 12.0 and higher and no service finger for earlier version, is included.

JUNOS Procedure: Under the edit system services hierarchy enter a show command to verify that the finger command is not present.

Reference: DODI 8500.2 DCBP-1

Category: Service Configuration

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0890

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure HTTP and FTP services are disabled.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0900

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure BOOTP is disabled.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that the IOS command no ip bootp server is present.

JUNOS Procedure: JUNOS does not support the bootp or any other service to automatically copy or download images of JUNOS from a server or another router; hence, this will never be a finding.

Reference: DODI 8500.2 COBR-1, DCSQ-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0910

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure configuration auto-loading is disabled.

Procedure: IOS Procedure: Review all router configurations to ensure the commands boot network and service config are not included.

Note: Disabled by default in version 12.0 and higher so the commands no boot network and no service config will not be displayed in the running configuration.

JUNOS Procedure: JUNOS does not provide the ability to automatically load a configuration from another server on the network; hence, this will never be a finding. .

Reference: DODI 8500.2 COBR-1, DCSQ-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0920

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will disable IP source routing.

Procedure: IOS Procedure: Review all Cisco router configurations to ensure the command no ip source-route is included.

JUNOS Procedure: Under the edit chassis hierarchy enter a show command to verify that the no-source-route command is present on all Juniper routers.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0930

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will disable Proxy ARP.

Procedure: IOS Procedure: Review all router configurations to ensure the command no ip proxy-arp is included for every active interface.

JUNOS Procedure: JUNOS does not provide the ability to extend the network at layer 2 across multiple LAN segments via proxy ARP; hence, this will never be a finding.

Reference: DODI 8500.2 DCBP-1

Category: Service Configuration

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0940

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will disable Gratuitous ARP.

Procedure: IOS Procedure: Review all router configurations to ensure the command no ip gratuitous-arp is included for every active interface.

JUNOS Procedure: JUNOS does not provide the ability to extend the network at layer 2 across multiple LAN segments via gratuitous ARP; hence, this will never be a finding.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0950

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will disable IP directed broadcasts on all router interfaces.

Procedure: IOS Procedure: IP directed broadcast is disabled by default in IOS version 12.0 and higher so the command no ip directed-broadcast will not be displayed in the running configuration, verify that the running configuration does not contain the command ip directed-broadcast. For versions prior to 12.0 ensure the command no ip directed-broadcast is displayed in the running configuration. JUNOS Procedure:

JUNOS does not forward directed broadcasts; hence, this will never be a finding.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0960

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure the router is configured to not reply with an ICMP unreachable message if a packet is rejected by an ACL or a network route is unknown.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0970

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will disable IP redirects on all router interfaces.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0980

Severity: CAT II

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will disable ICMP mask replies on all router interfaces.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.3 - Router - Services

IPW0990

Severity: CAT III

STIG Ref:

5.4.3

Policy: The IP WAN router administrator will ensure a minimum of two DNS servers are configured on the router.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.4 - Router - Routing

IPW1000

Severity: CAT III

STIG Ref:

5.4.4

Policy: The IP WAN router administrator will ensure all routing updates sent and received on IAPIs, IRTIs, and EAPIs will be authenticated using an MD5 key, if supported by the current approved router software version.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.4.1 - Router - Route Authentication

IPW1005

Severity: CAT I

STIG Ref:

5.4.4.1

Policy: The IP WAN Router Administrator will ensure the lifetime of the MD5 Key expiration is set to never expire. The lifetime of the MD5 key will be configured as infinite for route authentication.

NOTE: If using a key chain, at least one key will be set to never expire.

Procedure: Review the router configuration to determine if route authentication is configured. If router authentication is not used, this will not be a finding. If route authentication IS used, verify that all router authentication keys are configured to never expire.

If a key chain is used (e.g., for EIGRP), verify that one of the keys is configured with an infinite lifetime and that the send and accept times are current.

Reference: DODI 8500.2 IAKM-2

Category: Expiration

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.4 - Router - Routing

IPW1010

Severity: CAT II

STIG Ref:

5.4.4

Policy: The IP WAN router administrator will ensure route integrity to subscribers using route authentication, static routing, or by configuring an access control list for subscriber networks attached to Subscriber Interfaces.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.5 - Router - Logging

IPW1020

Severity: CAT III

STIG Ref:

5.4.5

Policy: The IP WAN router administrator will ensure logging is enabled on all routers.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECAT-1, ECAT-2

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.5 - Router - Logging

IPW1030

Severity: CAT IV

STIG Ref:

5.4.5

Policy: The IP WAN router administrator will ensure the logging buffer level is configured to buffer debug messages.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECAR-1, ECAR-2, ECAR-3

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.5 - Router - Logging

IPW1040

Severity: CAT IV

STIG Ref:

5.4.5

Policy: The IP WAN router administrator will ensure the logging buffer size is equal to or greater than 16384 bytes if the router memory supports this setting.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECAT-1, ECAT-2

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.5 - Router - Logging

IPW1050

Severity: CAT III

STIG Ref:

5.4.5

Policy: The IP WAN router administrator will ensure console logging is disabled during normal operation.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.5 - Router - Logging

IPW1060

Severity: CAT III

STIG Ref:

5.4.5

Policy: The IP WAN router administrator will ensure timestamps are configured for logging messages. The time stamp will include the ms and time zone.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECAR-1, ECAR-2, ECAR-3

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.5 - Router - Logging

IPW1070

Severity: CAT III

STIG Ref:

5.4.5

Policy: The IP WAN router administrator will ensure log messages are logged to a syslog server.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECTB-1

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.5 - Router - Logging

IPW1080

Severity: CAT III

STIG Ref:

5.4.5

Policy: The IP WAN router administrator will ensure syslog messages are configured to log up to and including the information level (syslog severity code 6).

Procedure: 1. Reference the appropriate router checklist procedure guide to verify that it is sending log messages levels 0 through 6 to the syslog server.

2. Review the syslog server configuration to ensure it is collecting syslog messages levels 0 through 6 for the appropriate facilities (Cisco routers default to Local7).

Reference: DODI 8500.2 ECAR-1, ECAR-2, ECAR-3

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.6 - Router - SNMP

IPW1090

Severity: CAT II

STIG Ref:

5.4.6

Policy: The IP WAN router administrator will restrict SNMP access to the router to authorized IP addresses.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.6 - Router - SNMP

IPW1100

Severity: CAT II

STIG Ref:

5.4.6

Policy: The IP WAN router administrators will ensure SNMP is enabled in the read only mode and Read/Write is not enabled unless approved by the IAO.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.6 - Router - SNMP

IPW1110

Severity: CAT I

STIG Ref:

5.4.6

Policy: The IAO will ensure the private and public community names are changed from the default values and that they are created IAW the DODI 8500.2 password IA Controls (IAIA-1, IAIA-2).

Procedure: Interview the IAO.

Reference: DODI 8500.2 IAIA-1, IAIA-2

Category: Passwords

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.7 - IRouter - nterfaces

IPW1120

Severity: CAT III

STIG Ref:

5.4.7

Policy: IP WAN router administrators will disable router interfaces that are not in use.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECND-1, ECND-2

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.7 - IRouter - nterfaces

IPW1130

Severity: CAT IV

STIG Ref:

5.4.7

Policy: The IP WAN router administrators will ensure a description is configured on each active router interface IAW the Program Management Office's Interface Description standard procedure and suffix the description with the interface type (i.e., suffix with IRTI, IAPI, EAPI, or SI).

Procedure: Review the router configurations and verify that all active interfaces have a description.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.7 - IRouter - nterfaces

IPW1140

Severity: CAT II

STIG Ref:

5.4.7

Policy: The IP WAN router administrator will ensure each active interface has the appropriate ACL applied.

Procedure: Review the router configurations and verify that all active interfaces have the appropriate ACL applied.

Reference: DODI 8500.2 DCP-1, DCBP-1

Category: Filters/Wrappers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1150

Severity: CAT II

STIG Ref:

5.4.8

Policy: The IP WAN router administrator will ensure data network routers are not configured to use modems (this does not include OOBM terminal servers).

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECND-1, ECND-2

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1160

Severity: CAT III

STIG Ref:

5.4.8

Policy: The IP WAN router administrators will ensure user authentication attempts (successful and unsuccessful) on the VTY lines are logged.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECAT-1, ECAT-2

Category: Inadequate Audit Trails

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1170

Severity: CAT III

STIG Ref:

5.4.8

Policy: The IP WAN router administrator will configure the VTY ports to time out after ten minutes of inactivity.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECND-1, ECND-2

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1180

Severity: CAT II

STIG Ref:

5.4.8

Policy: The IP WAN router administrator will configure the VTY ports to only use SSH transport on inbound terminal sessions during normal operation.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECNK-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1190

Severity: CAT III

STIG Ref:

5.4.8

Policy: The IP WAN router administrator will configure the VTY ports to use AAA services under normal or default operation.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 IAAC-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1200

Severity: CAT II

STIG Ref:

5.4.8

Policy: The IP WAN router administrator will ensure network access to the VTY line is restricted to authorized management devices (i.e., management work station, communication server device-management IP pool)

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECND-1, ECND-2

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1210

Severity: CAT III

STIG Ref:

5.4.8

Policy: IP WAN router administrators will ensure the router CON port is configured to time out after fifteen minutes or less of inactivity.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECND-1, ECND-2

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1220

Severity: CAT II

STIG Ref:

5.4.8

Policy: The IP WAN router administrator will ensure the console port is configured to authenticate users with AAA services under normal or default operation.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 IAAC-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.8 - Router - Lines

IPW1230

Severity: CAT III

STIG Ref:

5.4.8

Policy: IP WAN router administrators will ensure the router's auxiliary port is disabled and will not be used for remote administration unless approved by the PMO (i.e., transport input none, exec-timeout 0 1).

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECND-1, ECND-2

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1240

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will restrict SNMP traffic destined for the router to authorized SNMP servers.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1250

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will restrict SSH traffic destined for the router to authorized SSH clients.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1260

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will restrict access to the VTY port to authorized network management devices.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECND-1, ECND-2

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1270

Severity: CAT III

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will configure the routers to only accept NTP traffic from authorized NTP servers.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1280

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will ensure the most current GNSC directed Internet Access Point ACL is applied so that all traffic to/from the Internet is filtered using the ACL.

NOTE: This can be accomplished using a dedicated filter router.

Procedure: Review the router configurations and verify that all active interfaces have the appropriate ACL applied.

Reference: DODI 8500.2 DCP-1, DCBP-1

Category: Filters/Wrappers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1290

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrators will comply with the GNSC instructions on implementing exceptions to the IAPI ACLs.

Procedure: Review the router configurations and verify that all active interfaces have the appropriate ACL applied and have followed GNSC instructions on implementing exceptions to the IAPI ACLs.

Reference: DODI 8500.2 DCP-1, DCBP-1

Category: Filters/Wrappers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1300

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will apply the default ACL requirements to the IRTIs.

Procedure: Review the router configurations and verify that all IRTIs have the default ACL applied.

Reference: DODI 8500.2 DCP-1, DCBP-1

Category: Filters/Wrappers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1310

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will ensure SI interfaces block traffic destined for the IP WAN network backbone or management IP address space, with the exception of approved network troubleshooting port, protocols, and services (i.e., ICMP echo request and echo reply might be permitted to a SI IP address from a directly connected subscriber).

Procedure: Review the router configurations and verify that all subscriber interfaces have the appropriate ACL applied.

Reference: DODI 8500.2 DCP-1, DCBP-1

Category: Filters/Wrappers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9.4 - Router - Subscriber Interface (SI) ACL

IPW1315

Severity: CAT II

STIG Ref:

5.4.9.4

Policy: The IP WAN router administrator will ensure SI interfaces are configured with ingress and egress access control lists to restrict traffic based on the IP addresses that are approved for the connecting subscriber.

Procedure: Verify that the subscriber interface is configured to protect the customer and the IP WAN from spoofed traffic. To satisfy this requirement, the router subscriber interface should be configured with ingress and egress ACLs based on the IP Address ranges of the connected subscriber.

NOTE: This may also be accomplished on the ingress by using unicast Reverse Path Forwarding and on the egress by using configured route filters or static routes.

Reference: DODI 8500.2 ECIC-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9.4 - Router - Subscriber Interface (SI) ACL

IPW1316

Severity: CAT III

STIG Ref:

5.4.9.4

Policy: The IP WAN network administrator will ensure Unicast RPF is implemented on subscriber interfaces.

Procedure: Verify routers are configured to use uRPF on subscriber interfaces.

NOTE: If the router is configured with restrictive ACLs based on the connected subscriber IP Addresses, then this check should not be a finding. Refer to IPW1315.

Reference: DODI 8500.2 ECIC-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1320

Severity: CAT III

STIG Ref:

5.4.9

Policy: The IP WAN Router Administrator will block all BOGON networks from traversing the IP WAN, with the exception of approved IP WAN backbone or management network IP Address space. The IP WAN Router Administrator will check for changes and modify the BOGON list on a monthly basis.

Procedure: Review the router configurations and verify that the all Sis, IAPIs, and EAPIs are blocking packets with BOGON addresses.

Reference: DODI 8500.2 DCP-1, DCBP-1

Category: Filters/Wrappers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.9 - Router - ACL

IPW1330

Severity: CAT II

STIG Ref:

5.4.9

Policy: The IP WAN router administrator will ensure all well-known DDoS attack ports are blocked on all IAPIs and EAPIs.
* TCP - 2222, 6669, 6711-6712, 6776, 7000, 16660, 27665, 33270, 39168, 47017, 65000.
* UDP - 31335, 27444, 31337

Procedure: Review the router configurations and verify that the all SIs and IRTIs are blocking packets with DDoS attack ports.

Reference: DODI 8500.2 DCP-1, DCBP-1

Category: Filters/Wrappers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.10 - Router - Hostname

IPW1340

Severity: CAT III

STIG Ref:

5.4.10

Policy: The IP WAN router administrator will ensure each router is configured with a unique host name IAW IP WAN PMO naming standards.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that the IOS global command hostname is configured.

JUNOS Procedure: Review all Junos router configurations under the system hierarchy to verify that the hostname command configured.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.10 - Router - Hostname

IPW1350

Severity: CAT II

STIG Ref:

5.4.10

Policy: The IP WAN Router Administrator will ensure SSH is used to remotely connect to the router for management using the most current approved version of SSH (currently patched version 1.5 or higher)

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 ECKN-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.12 - Router - Secure Copy Protocol (SCP)

IPW1360

Severity: CAT III

STIG Ref:

5.4.12

Policy: The IP WAN router administrator will ensure SCP is used to transfer files to and from the router if supported by the PMO approved software version.

Procedure: Interview the IAO and router administrator. Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.13 - Router - FTP

IPW1370

Severity: CAT III

STIG Ref:

5.4.13

Policy: The IP WAN router administrator will configure each router to send an exception dump to an FTP server in the event of a router failure or crash.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.13 - Router - FTP

IPW1380

Severity: CAT II

STIG Ref:

5.4.13

Policy: The IP WAN router administrators will ensure the router is configured to use an FTP user and password to connect to FTP servers.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Configuration Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.13 - Router - FTP

IPW1390

Severity: CAT IV

STIG Ref:

5.4.13

Policy: The IP WAN router administrator will configure the routers to use FTP in active mode only.

Procedure: IOS Procedure: Review all Cisco router configurations to verify that the IOS global command no ip ftp passive (the default) is configured or that ip ftp passive is not configured.

JUNOS Procedure: NA

Reference: DODI 8500.2 DCBP-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.14 - Router - Network Time Protocol (NTP)

IPW1400

Severity: CAT II

STIG Ref:

5.4.14

Policy: The IP WAN router administrator will ensure each router is configured to use two PMO approved NTP servers.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Routers

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.14 - Router - Network Time Protocol (NTP)

IPW1410

Severity: CAT IV

STIG Ref:

5.4.14

Policy: The IP WAN router administrator will ensure NTP messages are authenticated using an MD5 key.

Procedure: Reference the appropriate router checklist procedure guide.

Reference: DODI 8500.2 DCBP-1

Category: Access Controls

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.14 - Router - Network Time Protocol (NTP)

IPW1420

Severity: CAT III

STIG Ref:

5.4.14

Policy: The IP WAN router administrator will ensure the router is configured to use the GMT time zone.

Procedure: IOS Procedure: The router configuration should have the following global command defined: clock timezone GMT 0

JUNOS Procedure: There should be either system time-zone UTC defined or no system time-zone statement as the default is Coordinated Universal Time (UTC)-- formerly known as Greenwich Mean Time.

Reference: DODI 8500.2 DCBP-1

Category: Network and Communications Security

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.15 - Router - Banner

IPW1430

Severity: CAT III

STIG Ref:

5.4.15

Policy: The TNC will ensure warning banners are displayed on all devices regardless of the access method. (i.e., SSH, ftp, https).

Procedure: Review the router configuration..

Reference: DODI 8500.2 ECWM-1

Category: Host Access Warning Message

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

5.4.15 - Router - Banner

IPW1440

Severity: CAT III

STIG Ref:

5.4.15

Policy: The IAO will ensure approved warning banners are configured on each IP WAN device. (Refer to CJCSM 6510.01, Enclosure C, Appendix C, for an example).

Procedure: Review the router configuration.

Reference: DODI 8500.2 ECWM-1

Category: Host Access Warning Message

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

6.2 - Network Operation Center

IPW1480

Severity: CAT II

STIG Ref:

6.2

Policy: The IP WAN PMO will ensure a COOP is developed, maintained, and exercised on an annual basis to ensure continuous operational services of the IP WAN.

Procedure: Interview the IP WAN PMO, TNC IAO, and the GNSC IAO. Review the COOP plan documentation.

Reference: DODI 8500.2 CODP-1, CODP-2, CODP-3

Category: COOP/DRP

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES:

6.2 - Network Operation Center

IPW1490

Severity: CAT II

STIG Ref:

6.2

Policy: The IP WAN PMO will ensure the COOP plan establishes procedures for a smooth transition of mission essential IP WAN functions to include, management, operation, and monitoring.

Procedure: Interview the IP WAN PMO and review the COOP plan documentation.

Reference: DODI 8500.2 CODP-1, CODP-2, CODP-3

Category: COOP/DRP

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

NOTES: